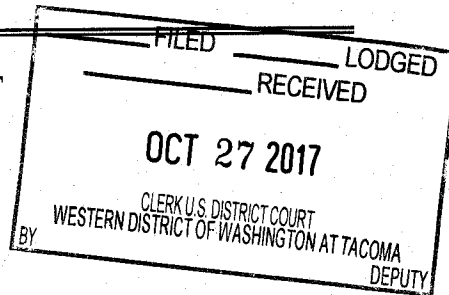


UNITED STATES DISTRICT COURT

for the
Western District of Washington



In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

One (1) Toshiba laptop computer, SN PSAGCU-06015 located
at Washington State Patrol Evidence System High Tech Crimes
Unit, 210 11th Ave. SW, Suite 402, Olympia, WA 98504

Case No.

MJ17-5188

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 245	Violation of federally protected activities
18 U.S.C. § 844(e)	Violation of interstate bomb threats
18 U.S.C. § 875(c)	Violation of interstate communications

The application is based on these facts:

See Affidavit of Patrick D. Dospoy

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

PATRICK D. DOSPOY, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/27/17

City and state: Tacoma, Washington

Judge's signature

J. RICHARD CREATURA, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF PIERCE)

I, Patrick D. Dospoy, having been duly sworn, state as follows:

Introduction And Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a digital device¹ or other electronic storage media,² hereinafter the “**Subject Device**,” which is currently in law enforcement possession, and the extraction from those devices or electronic storage media of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been since March 2017. Prior to the joining the FBI I obtained an undergraduate degree in biological sciences at the University of Chicago, I then obtained a doctorate in biomedical sciences from University of Texas Southwestern Medical Center and thereafter worked with at GPG, a venture capital firm. I received approximately 21 weeks of training at the FBI Academy in Quantico, Virginia where I was trained in legal processes and standards as well as investigative

¹ “Digital device” includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 techniques. I was assigned to the Tacoma RA, Seattle Division, South Sound Child
2 Exploitation Task Force. I work child pornography, sex trafficking, sexual assault,
3 and parental kidnapping cases.

4 3. The facts set forth in this Affidavit are based on my own personal
5 knowledge; knowledge obtained from other individuals during my participation in
6 this investigation, including other law enforcement officers; review of documents
7 and records related to this investigation; communications with others who have
8 personal knowledge of the events and circumstances described herein; and
9 information gained through my training and experience.

10 4. Because this Affidavit is submitted for the limited purpose of
11 establishing probable cause in support of the application for a search warrant, it does
12 not set forth every fact that I, or others, have learned during the course of this
13 investigation. I have set forth only the facts that I believe are necessary to establish
14 probable cause to believe that evidence and instrumentalities of violations of 18
15 U.S.C. §§ 245 (Interference with Federally Protected Rights), 844(e) (Interstate
16 Bomb Threats), and 875(c) (Interstate Threats), will be found on the **Subject Device**

17 **Identification Of The Subject Device To Be Examined**

18 5. The **Subject Device** is a Toshiba laptop computer, Model Number
19 PSAGCU-0601S, Serial Number 98669877Q ("Target Computer"), as more fully
20 described in Attachment A.

21 6. The **Subject Device** is contained in a black computer bag with a mouse
22 and power cord, and is currently located at the Washington State Patrol Evidence
23 System High Tech Crimes Unit, 210 11th Avenue SW, Suite 402, Olympia,
24 Washington 98504.

25 7. In my training and experience, I know that the **Subject Device** has been
26 stored in a manner in which its contents are, to the extent material to this
27 investigation, in substantially the same state as they were when the **Subject Device**
28 first came into the possession of the WSP.

1 8. The warrant would authorize the forensic examination of the **Subject**
2 **Device** for the purpose of identifying electronically stored data particularly
3 described in Attachment B.

4 **The Investigation of Ronald Nelson**

5 9. The FBI initiated an investigation into Ronald Nelson based on its
6 belief that he had sent Kevin Beiser is a Board Member of the San Diego Unified
7 School District, in the Southern District of California a threatening message.

8 10. In 2017, Mr. Beiser voted to support lesson plans to teach an overview
9 of various religions, including Islam, at San Diego public schools.

10 11. On approximately April 27, 2017, a person identified as “Ronald
11 Sandberg” posted a series of messages on Mr. Beiser’s Facebook page. The first
12 message was as follows:

13 *Just tried calling you at home Kevin, guess you were not home. Looking*
14 *forward to “getting in touch” soon. I promise you that we will cross*
15 *paths soon. [smiley face emoji]*

16 12. The second message, posted shortly thereafter, was as follows:

17 *In case anybody is interested in that lead board member of the San*
18 *Diego school district that wants our kids to to [sic] succumb to Sharia*
19 *Law and do Islamic prayers in class, his name is Kevin Richard Beiser.*
 He lives at [address omitted]. His landline telephone number is
 [telephone number omitted]. Have at him boys. [smiley face emoji]

20 The second posted message included Beiser’s correct home address, but incorrect
21 home telephone number.

22 13. In a third message, the poster wrote, “*No worries if none of you have*
23 *the chance to meet Kevin, I sure will soon. [smiley face emoji].”*

24 14. In the fourth message, the poster wrote, “*Wonders now if Kevin wishes*
25 *he had never left Bremerton lol (Laugh Out Loud) [smiley face emoji].”* Mr. Beiser
26 had previously lived in Bremerton, Washington.
27
28

1 15. Finally, the poster wrote, *"By the way, Kevin, just in case you think this*
2 *is a joke . . . you can run, but you can't hide. We will find you eventually. You had*
3 *better be looking over your shoulder from now on, we are right behind you."*

4 16. On May 4, 2017, San Diego Police Department ("SDPD") officers
5 interviewed Mr. Beiser at his home. Mr. Beiser was very upset and fearful. He
6 explained he was very afraid that anyone could show up at his home with the intent
7 to harm him or his husband because his home address was posted on Facebook. FBI
8 Agents interviewed Mr. Beiser on July 24, 2017, at which time he reiterated the
9 same ongoing fear.

10 17. Upon conducting a check of publicly-available information, an SDPD
11 officer reviewed the Facebook page of "Ronald Sandberg." The Facebook page
12 reflected that "Sandberg" lived in Anacortes, Washington. Upon conducting a
13 search of criminal history of "Sandburg," the officer noted that he shared the same
14 birthdate as Nelson.

15 18. A review of "Sandberg's" Facebook page indicates it is located at
16 www.facebook.com/ronald.nelson.980.

17 19. A review of Ronald Nelson's Washington State driver's license
18 revealed that he, like "Sandberg," lives in Anacortes, Washington, and his
19 photograph resembled the profile picture on "Sandberg's" Facebook page.

20 20. Anacortes and Bremerton, Washington are both located on islands near
21 Seattle, Washington. Bremerton is west of Seattle, and Anacortes is approximately
22 91.6 miles north of Bremerton.

23 21. On October 3, 2017, United States Magistrate Judge Nita L. Stormes,
24 Southern District of California, issued a search warrant (17MJ3668) for the
25 Facebook account of Ronald Nelson (aka Ronald Sandberg), based on the above.

26 22. On October 3, 2017, after obtaining a search warrant for Nelson's
27 Facebook account, FBI agents learned that Nelson's Computer (the **Subject Device**)
28 was in the possession of the Washington State Patrol (hereafter WSP).

1 **A. Skagit County Case**

2 23. Subsequent investigation revealed that on June 6, 2017, the Office of
3 the Governor of Washington contacted the WSP Criminal Investigation Unit
4 regarding a threatening email received through the Governor's web email (i.e. email
5 submitted to the Governor through his website). The email provided the following:

6 *Governor, I am giving you one week to solve the crises that is*
7 *happening at Evergreen State College in Olympia. If you decide to not*
8 *take care of it, I will be forced to use the powers that be in my group to*
9 *come after you personally and also the college there. Trust me*
10 *governor, you don't want to say no to this. Your very life depends on it.*
11 *Do the right thing and stop the nonsense at Evergreen, or else I am*
12 *personally going to come and find you, I am an ex-Marine. Trust me*
13 *gov, you DON'T want me to catch up with you. You have my full name*
14 *and address here so take this to heart, you fuck up on this, I will come*
15 *after you.*

16 Also included in the email was Nelson's name, address, and telephone number. The
17 email originated from Ronald.Nelson@msn.com ("Nelson's email address").

18 24. WSP officers reviewed the email and identified Nelson's address as
19 XXXXX Avenue, Anacortes, Washington ("Nelson's residence address"). Using
20 publicly-available information, officers searched Facebook using Nelson's email
21 address, and located the Facebook page with the vanity name "Ronald Sandberg."

22 25. The Washington Governor's Office provided WSP officers with
23 information of the email sent from Nelson's email address, including the Internet
24 Protocol ("IP") number from which it originated. Using an open source website that
25 identifies the origin of IP addresses, WSP officers learned the IP address was
26 provided by Frontier Communications, located in Skagit County, Washington.
27 Anacortes is located in Skagit County. Officers subsequently obtained a Washington
28 State search warrant for the IP address and learned it was issued to Nelson's
residence address.

29 26. At approximately 8:30 p.m., June 6, 2017, WSP officers responded to
Nelson's residence. Nelson's wife answered the door and explained Nelson was in

1 the shower. Officers were granted permission to go inside to wait for Nelson.
2 Officers stood at the door and declined the invitation to enter further. Mrs. Nelson
3 explained they share the residence with Nelson's brother, his wife, and their son.

4 27. After a few minutes, Nelson came to the door of his residence where
5 officers were waiting. When told officers were there to discuss his recent
6 communication with the Governor's Office, Nelson's left cheek made a distinct
7 twitch and Nelson looked down and away, appearing very nervous.

8 28. Nelson initially told officers he was drunk the night before and did not
9 remember what he had done. Officers asked if he would voluntarily accompany
10 them for an interview. Nelson consented and asked if he could first change his
11 clothing.

12 29. While waiting for Nelson to change clothes, officers observed the
13 **Subject Device** on the dining room table. Mrs. Nelson stated it belonged to Nelson,
14 which Nelson subsequently confirmed. Officers asked Nelson for permission to take
15 the **Subject Device** with him to the interview, and Nelson agreed.

16 30. At the Anacortes Police Department, officers advised Nelson of his
17 *Miranda* rights. Nelson confirmed that he understood his rights and consented to an
18 audio-recorded interview.

19 31. When asked about the email to the Governor's Office, Nelson said,
20 "well, I know one thing I need to do is stop drinking so much." Although he
21 initially claimed he did not recall the communication, Nelson said "I'm not saying I
22 didn't . . . I think it is possible . . . it had to be me." Nelson also confirmed he did
23 not think it was possible for anyone else in his household to contact the Governor's
24 Office from his computer. Finally, Nelson admitted the email came from him, that
25 he was online the night before, and recalled some of his communication with the
26 Governor's Office.

1 32. Nelson admitted he was angry the night before because he believed a
2 professor at Evergreen State College was being treated unfairly for allegedly losing
3 his job after refusing to leave campus on “no whites day.”

4 33. When asked how he would interpret his email, Nelson said, “the
5 ramblings of a madman,” and that it was “obviously” a threatening statement.

6 34. Nelson also informed officers that he had previously been interviewed
7 by Secret Service Agents in 2011, after he sent a message to President Obama that
8 “I’d like to get him in my sights.”

9 35. Nelson explained that, although he had rebuilt the **Subject Device**
10 several months ago, he did not manually erase his computer’s browser history, and
11 does not erase cookies. When told that officers would apply for a warrant to search
12 the **Subject Device**, and asked if there was anything in addition to that pertaining to
13 the immediate investigation, Nelson said, “No, you’re free to -- free to do that if you
14 like, so I don’t – I don’t have anything to hide.”

15 36. As a result of their investigation, Nelson was charged in Skagit County
16 District and Municipal Court with misdemeanor Harassment in violation of Revised
17 Code of Washington, 9A.46.020.

18 37. On June 20, 2017, WSP officers obtained a search warrant to search the
19 **Subject Device**. They obtained information from the **Subject Device** but did not
20 review it because Nelson’s pled guilty on August 7, 2017. The Skagit County
21 District and Municipal Court sentenced Nelson to 364 days of jail (with 350 days
22 suspended), followed by 24 months of probation, and a fine of \$5,000.

23 38. The **Subject Device** remains in the custody of the WSP, but they intend
24 to return it to Nelson soon due to the termination of State criminal proceedings.

25 39. Despite his conviction in Skagit County District Court and Municipal
26 Court, Nelson remains the target of an investigation in the Southern District of
27 California for the crimes outlined in Attachment B.
28

40. Based on my training and experience, I use the following technical terms to convey the following meanings:

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

Computers, Electronic Storage, And Forensic Analysis

42. Based on my knowledge, training, and experience, I know that digital devices and electronic storage media can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device used to access the internet. This information can sometimes be recovered with forensic tools.

1 43. There is probable cause to believe that things that were once stored on
2 some of the **Subject Device** may still be stored there, for at least the following
3 reasons:

4 a. Based on my knowledge, training, and experience, I know that
5 computer files or remnants of such files can be recovered months or even years after
6 they have been downloaded onto a storage medium, deleted, or viewed via the
7 Internet. Electronic files downloaded to a storage medium can be stored for years at
8 little or no cost. Even when files have been deleted, they can be recovered months or
9 years later using forensic tools. This is so because when a person "deletes" a file on
a computer, the data contained in the file does not actually disappear; rather, that
data remains on the storage medium until it is overwritten by new data.

10 b. Therefore, deleted files, or remnants of deleted files, may reside
11 in free space or slack space – that is, in space on the storage medium that is not
12 currently being used by an active file – for long periods of time before they are
overwritten. In addition, a computer's operating system may also keep a record of
deleted data in a "swap" or "recovery" file.

13 c. Wholly apart from user-generated files, computer storage media
14 – in particular, computers' internal hard drives – contain electronic evidence of how
15 a computer has been used, what it has been used for, and who has used it. To give a
16 few examples, this forensic evidence can take the form of operating system
17 configurations, artifacts from operating system or application operation, file system
18 data structures, and virtual memory "swap" or paging files. Computer users typically
do not erase or delete this evidence, because special software is typically required
for that task. However, it is technically possible to delete this information.

19 d. Similarly, files that have been viewed via the internet are
20 sometimes automatically downloaded into a temporary Internet directory or "cache."

21 44. *Forensic evidence.* As further described in Attachment B, this
22 application seeks permission to locate not only electronically stored information that
23 might serve as direct evidence of the crimes described on the warrant, but also
24 forensic evidence that establishes how the **Subject Device** were used, the purpose of
25 their use, who used them, and when. There is probable cause to believe that this
26 forensic electronic evidence might be on the **Subject Device** because:

27 a. Data on the storage medium can provide evidence of a file that
28 was once on the storage medium but has since been deleted or edited, or of a deleted

1 portion of a file (such as a paragraph that has been deleted from a word processing
2 file). Virtual memory paging systems can leave traces of information on the storage
3 medium that show what tasks and processes were recently active. Web browsers, e-
4 mail programs, and chat programs store configuration information on the storage
5 medium that can reveal information such as online nicknames and passwords.
6 Operating systems can record additional information, such as the attachment of
7 peripherals, the attachment of USB flash storage devices or other external storage
8 media, and the times the computer was in use. Computer file systems can record
9 information about the data files that were created and the sequence in which they
10 were created.

11 b. As explained herein, information stored within a computer and
12 other electronic storage media may provide crucial evidence of the “who, what, why,
13 when, where, and how” of the criminal conduct under investigation, thus enabling
14 the United States to establish and prove each element or alternatively, to exclude the
15 innocent from further suspicion. In my training and experience, information stored
16 within a digital device such as a cell phone (e.g., registry information,
17 communications, images and movies, transactional information, records of session
18 times and durations, internet history, and anti-virus, spyware, and malware detection
19 programs) can indicate who has used or controlled the computer or storage media.
20 This “user attribution” evidence is analogous to the search for “indicia of
21 occupancy” while executing a search warrant at a residence. The existence or
22 absence of anti-virus, spyware, and malware detection programs may indicate
23 whether the device was remotely accessed, thus inculcating or exculpating the
24 device owner and/or others with direct physical access to the device. Further,
25 computer and storage media activity can indicate how and when the device was
26 accessed or used. For example, as described herein, typically contain information
27 that log: computer user account session times and durations, computer activity
28 associated with user accounts, electronic storage media that connected with the
computer, and the IP addresses through which the computer accessed networks and
the internet. Such information allows investigators to understand the chronological
context of computer or electronic storage media access, use, and events relating to
the crime under investigation. Additionally, some information stored within a
computer or electronic storage media may provide crucial evidence relating to the
physical location of other evidence and the suspect. The existence of such image
files, along with external device connection logs, may also indicate the presence of
additional electronic storage media (e.g., a digital camera or cellular phone with an
incorporated camera). Last, information stored within a device may provide relevant
insight into the device user’s state of mind as it relates to the offense under
investigation. For example, information within the device may indicate the owner’s
motive and intent to commit a crime (e.g., internet searches indicating criminal
planning), or consciousness of guilt (e.g., running a “wiping” program to destroy
evidence on the computer or password protecting/encrypting such evidence in an
effort to conceal it from law enforcement).

1 c. A person with appropriate familiarity with how an electronic
2 device works may, after examining this forensic evidence in its proper context, be
3 able to draw conclusions about how electronic devices were used, the purpose of
4 their use, who used them, and when.

5 d. The process of identifying the exact electronically stored
6 information on a storage medium that are necessary to draw an accurate conclusion
7 is a dynamic process. Electronic evidence is not always data that can be merely
8 reviewed by a review team and passed along to investigators. Whether data stored on
9 a computer is evidence may depend on other information stored on the computer and
10 the application of knowledge about how a computer behaves. Therefore, contextual
11 information necessary to understand other evidence also falls within the scope of the
12 warrant.

13 e. Further, in finding evidence of how a device was used, the
14 purpose of its use, who used it, and when, sometimes it is necessary to establish that
15 a particular thing is not present on a storage medium.

16 45. *Manner of execution.* Because this warrant seeks only permission to
17 examine a device already in law enforcement's possession, the execution of this
18 warrant does not involve the physical intrusion onto a premises. Consequently, I
19 submit there is reasonable cause for the Court to authorize execution of the warrant
20 at any time in the day or night.

21 Digital Devices As Instrumentalities Of The Crime

22 46. As described above Nelson has actively used his online accounts to
23 make threats against others.

24 47. Based on my training and experience, and through consultations with
25 other law enforcement agents experienced in the investigation of hate crimes and
26 interstate threat offenses, I know that evidence of motivation of persons involved in
27 hate crimes and interstate threat offenses can assist in the identification of the
28 subject, co-conspirators, and victims. I know that one study identifies four broad
categories of hate crime offenders and their typical motivations; 1) thrill offenders –
who commit their crimes for the excitement or the thrill; 2) defensive offenders –
who view themselves as defending their "turf"; 3) mission offenders – who believe
their life's mission is to rid the world of groups they consider evil or inferior; and, 4)

1 retaliatory offenders – who engage in retaliatory violence in the belief that by doing
2 so, just desserts is served.³

3 48. Based on my training and experience, and through consultations with
4 other law enforcement agents in the investigation of hate crimes and interstate threat
5 offenses, I know that persons involved in hate crimes and interstate threat offenses
6 use computers for the following reasons:

7 a. to collect, produce, and store (for at least one year) word
8 processing documents, records, messages (including electronic mail (“email”) and
9 text messages), images, or data, that tend to show motivation and beliefs that give
10 rise to hate crime offenses or threatening behavior and statements;

11 b. to communicate with others (including both targets and persons
12 with whom they share beliefs and opinions) via messages, online group chats, social
13 media, websites (including news comment sections), that tend to show motivation
14 and beliefs that give rise to hate crime offenses, or threatening behavior and
15 statements;

16 c. to visit internet websites of persons or groups that they believe
17 share their motivation and beliefs that give rise to hate crime offenses, or threatening
18 behavior and statements; and,

19 d. to visit internet websites of persons or groups who are targets of
20 their motivation and beliefs that give rise to hate crime offenses, or threatening
21 behavior and statements.

22 Search Techniques

23 49. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the
24 Federal Rules of Criminal Procedure, the warrant I am applying for will permit
25 imaging or otherwise copying all data contained on the **Subject Device**, and will
26

27 ³ McDevitt, J., Levin, J. and Bennett, S. (2002). “Hate Crime offenders: an expanded
28 typology,” Journal of Social Issues 58/2:303-17.

1 specifically authorize a review of the media or information consistent with the
2 warrant.

3 50. In accordance with the information in this affidavit, law enforcement
4 personnel will execute the search of the **Subject Device** pursuant to this warrant as
5 follows:

6 **a. Securing the Data**

7 i. In order to examine the ESI in a forensically sound
8 manner, law enforcement personnel with appropriate expertise will attempt to
9 produce a complete forensic image, if possible and appropriate, of the Subject
Device⁴

10 ii. Law enforcement will only create an image of data
11 physically present on or within the **Subject Device**. Creating an image of the
12 **Subject Device** will not result in access to any data physically located elsewhere.
However, **Subject Device** that have previously connected to devices at other
locations may contain data from those other locations.

13 **b. Searching the Forensic Images**

14 i. Searching the forensic images for the items described in
15 Attachment B may require a range of data analysis techniques. In some cases, it is
16 possible for agents and analysts to conduct carefully targeted searches that can locate
17 evidence without requiring a time-consuming manual search through unrelated
18 materials that may be commingled with criminal evidence. In other cases, however,
19 such techniques may not yield the evidence described in the warrant, and law
20 enforcement may need to conduct more extensive searches to locate evidence that
21 falls within the scope of the warrant. The search techniques that will be used will be
only those methodologies, techniques and protocols as may reasonably be expected
to find, identify, segregate and/or duplicate the items authorized to be seized
pursuant to Attachment B to this affidavit.

22 ⁴ The purpose of using specially trained computer forensic examiners to conduct the imaging of
23 digital devices or other electronic storage media is to ensure the integrity of the evidence and to
24 follow proper, forensically sound, scientific procedures. When the investigative agent is a trained
25 computer forensic examiner, it is not always necessary to separate these duties. Computer
26 forensic examiners often work closely with investigative personnel to assist investigators in their
27 search for digital evidence. Computer forensic examiners are needed because they generally have
28 technological expertise that investigative agents do not possess. Computer forensic examiners,
however, often lack the factual and investigative expertise that an investigative agent may
possess on any given case. Therefore, it is often important that computer forensic examiners and
investigative personnel work closely together.


1 ii. Agents may utilize hash values to exclude certain known
2 files, such as the operating system and other routine software, from the search
3 results. However, because the evidence I am seeking does not have particular
4 known hash values, agents will not be able to use any type of hash value library to
locate the items in Attachment B.

5 Request For Sealing

6 51. It is respectfully requested that this Court issue an order sealing, until
7 further order of the Court, all papers submitted in support of this application,
8 including the application and search warrant. I believe that sealing this document is
9 necessary because the warrant is relevant to an ongoing investigation. Based upon
10 my training and experience, I have learned that, online criminals actively search for
11 criminal affidavits and search warrants via the internet, and disseminate them to
12 other online criminals as they deem appropriate, i.e., post them publicly online
13 through the carding forums. Premature disclosure of the contents of this affidavit
14 and related documents may have a significant and negative impact on the continuing
15 investigation and may severely jeopardize its effectiveness.

16 Conclusion

17 52. I submit that this affidavit supports probable cause for a search warrant
18 authorizing the examination of the **Subject Device** described in Attachment A to
19 seek the items described in Attachment B.

20
21
22 
23 PATRICK D. DOSPOY
Special Agent, FBI

24 Subscribed and sworn to before me this 27th day of October, 2017.

25
26
27 
28 J. RICHARD CREATURA
United States Magistrate Judge

ATTACHMENT A

The **Subject Device** is a Toshiba laptop computer, Model Number PSAGCU-0601S, Serial Number 98669877Q ("Target Computer"). The **Subject Device** is contained in a black computer bag with a mouse and power cord, and is currently located at the Washington State Patrol Evidence System High Tech Crimes Unit, 210 11th Avenue SW, Suite 402, Olympia, Washington 98504.

This warrant authorizes the forensic examination of the **Subject Device** for the purpose of identifying the electronically stored information described in Attachment B.

As soon as practicable, but in any event no later than within 60 days of seizure (absent further order of the issuing judicial officer), the government must provide the issuing judicial officer with a return containing a sworn certificate that:

- (a) certifies precisely what ESI it has obtained;
- (b) certifies what ESI it has returned;
- (c) certifies it has returned the actual device(s) seized; and
- (d) certifies it has destroyed any copy made of the ESI that is outside the scope of the warrant.

Attachment B

All records on the **Subject Device** described in Attachment A that relate to violations of 18 U.S.C. §§ 245, 844(e), and/or 875(c) and involve Ronald Nelson since April 27, 2016 (approximately one year prior to the alleged offense(s)), including:

1. word processing documents, records, messages (including electronic mail ("email") and text messages), images, or data on "digital devices" (defined below):

a. collected, produced, or stored, that tend to show motivation and beliefs that give rise to hate crime offenses or threatening behavior and statements;

b. indicating communications with others via messages, online group chats, social media, websites, that tend to show motivation and beliefs that give rise to hate crime offenses, or threatening behavior and statements;

c. indicating visits to Internet websites of persons or groups that they believe share their motivation and beliefs that give rise to hate crime offenses, or threatening behavior and statements;

d. indicating visits to Internet websites of persons or groups who are targets of their motivation and beliefs that give rise to hate crime offenses, or threatening behavior and statements;

e. identifying or tending to identify other participants in the crimes above;

f. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of electronic information in (a)-(d) above.

2. Evidence of user attribution showing who used or owned the **Subject Device** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

1 As used above, the terms "records" and "information" include all of the
2 foregoing items of evidence in whatever form and by whatever means they may have
3 been created or stored, including any form of computer or electronic storage (such as
4 flash memory or other media that can store data) and any photographic form.